



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

M

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,759	03/24/2004	Jia-Bin Huang	REAP0062USA	2758
27765	7590	10/12/2007	EXAMINER	
NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION P.O. BOX 506 MERRIFIELD, VA 22116			BROWN, CHRISTOPHER J	
		ART UNIT	PAPER NUMBER	
		2134		
		NOTIFICATION DATE	DELIVERY MODE	
		10/12/2007	ELECTRONIC	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

winstonhsu.uspto@gmail.com
Patent.admin.uspto.Rcv@naipo.com
mis.ap.uspto@naipo.com.tw

Office Action Summary	Application No.	Applicant(s)
	10/708,759	HUANG, JIA-BIN
	Examiner	Art Unit
	Christopher J. Brown	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 24 March 2004.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-20 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 3/24/2004 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Objections

Claim 4 recites the limitation "the master list" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claims 16, and 20 state "update the decryption keys in the key-table according to the decryption key when the decryption key is not stored in the key-table" It is unclear if the applicant intended to state "according to the encrypted data" as in claims 1, and 10. Clarification would be appreciated.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-4, 6-11, 13-18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lin US 2005/0154871 in view of Bourk US 6,973,071 in view of Kim US 2003/0105717.

As per claim 1 Lin teaches receiving encrypted data from the sender (receive encrypted packet) [0018]. Lin teaches searching a key-table of the receiver for a decryption key corresponding to the encrypted data (search for Key ID in table 1 for secret key) [0018]. Lin teaches decrypting the encrypted data through utilizing the decryption key stored in the key-table (decrypt the received packet) [0018].

Lin fails to teach updating the key-table according to the encrypted data and enabling a re-transmission mechanism of the sender when the decryption key is not stored in the key-table;

Bourk teaches enabling retransmission mechanism by not transmitting an acknowledgement from the receiver to the transmitter (Col 10 lines 25-32).

It would have been obvious to one of ordinary skill in the art to enable retransmission because of an error in decryption or errors in data transmitted.

Kim teaches searching a key table (memory) for a key according to encrypted data [0038]. Kim teaches updating the key table according to the encrypted data (downloading a key from a database and storing the decryption key in memory) [0048] [0050].

It would have been obvious to one of ordinary skill in the art to use the decryption key update of Kim with the system of Lin, because it allows a receiver to utilize the incoming data rather than being forced to discard it.

As per claim 2, Lin teaches using a Media Access Control (MAC) Address of the sender to search the key-table for the decryption key (Uses check values Key ID, Address 1, and Address 2, to search for decryption key, where Address 2 is the transmitter MAC address) [0009], [0016], [0019].

As per claim 3, Lin teaches triggering a system interrupt to notify a controller of the receiver if the decryption key is not stored in the key-table (error message is sent to PC upon the key is not found) [0038].

As per claim 4, Lin teaches that the controller searches the master list for the decryption key and transfers the decryption key to the key-table when receiving the system interrupt (PC, CPU searches for the key on a website data base after an error is detected and stores the key in memory) [0038] [0046] [0048].

As per claim 6, Lin teaches discarding the encrypted data when the decryption key is not stored in the key-table (packet will be discarmer if nothing located for decapsulation) [0019].

As per claim 7, Lin fails to teach disabling the receiver from outputting an acknowledgement message to the sender to inform the sender of reception of the encrypted data.

Bourk teaches enabling retransmission mechanism by not transmitting an acknowledgement from the receiver to the transmitter (Col 10 lines 25-32). It would have been obvious to one of ordinary skill in the art to enable retransmission because of an error in decryption or errors in data transmitted.

As per claim 8, Lin teaches a wireless LAN (WLAN) system (WLAN environment) [0010].

As per claim 9, Lin teaches the receiver is a wireless network card inserted in a computer (WLAN enabled NIC) [0016].

As per claim 10, Lin teaches receiving encrypted data from the sender (receive encrypted packet) [0018]. Lin teaches searching a key-table of the receiver for a decryption key corresponding to the encrypted data (search for Key ID in table 1 for secret key) [0018]. Lin teaches decrypting the encrypted data through utilizing the decryption key stored in the key-table (decrypt the received packet) [0018].

Lin fails to teach updating the key-table according to the encrypted data and enabling a re-transmission mechanism of the sender when the decryption key is not stored in the key-table;

Bourk teaches enabling retransmission mechanism by not transmitting an acknowledgement from the receiver to the transmitter (Col 10 lines 25-32).

It would have been obvious to one of ordinary skill in the art to enable retransmission because of an error in decryption or errors in data transmitted.

Kim teaches searching a key table (memory) for a key according to encrypted data [0038]. Kim teaches updating the key table according to the encrypted data (downloading a key from a database and storing the decryption key in memory) [0048] [0050].

It would have been obvious to one of ordinary skill in the art to use the decryption key update of Kim with the system of Lin, because it allows a receiver to utilize the incoming data rather than being forced to discard it.

As per claim 11, Lin teaches using a Media Access Control (MAC) Address of the sender to search the key-table for the decryption key (Uses check values Key ID, Address 1, and Address 2, to search for decryption key, where Address 2 is the transmitter MAC address) [0009], [0016], [0019].

As per claim 13, Lin teaches a wireless LAN (WLAN) system (WLAN environment) [0010].

As per claim 14, Lin teaches discarding the encrypted data when the decryption key is not stored in the key-table (packet will be discarded if nothing located for decapsulation)

[0019].

As per claim 15, Lin fails to teach disabling the receiver from outputting an acknowledgement message to the sender to inform the sender of reception of the encrypted data. Lin teaches decrypting the encrypted data through utilizing the decryption key stored in the key-table (decrypt the received packet) [0018].

Bourk teaches enabling retransmission mechanism by not transmitting an acknowledgement from the receiver to the transmitter (Col 10 lines 25-32).

It would have been obvious to one of ordinary skill in the art to enable retransmission because of an error in decryption or errors in data transmitted:

As per claim 16, Lin teaches an apparatus with a receiver controller (CPU) and Network Interface Card (Host 110, CPU, NIC) [0007] Figure 1. Lin teaches receiving encrypted data from the sender (receive encrypted packet) [0018]. Lin teaches searching a key-table of the receiver for a decryption key corresponding to the encrypted data (search for Key ID in table 1 for secret key) [0018]. Lin teaches decrypting the encrypted data through utilizing the decryption key stored in the key-table (decrypt the received packet) [0018].

Lin fails to teach updating the key-table according to the encrypted data and enabling a re-transmission mechanism of the sender when the decryption key is not stored in the key-table;

Bourk teaches enabling retransmission mechanism by not transmitting an acknowledgement from the receiver to the transmitter (Col 10 lines 25-32).

It would have been obvious to one of ordinary skill in the art to enable retransmission because of an error in decryption or errors in data transmitted.

Kim teaches searching a key table (memory) for a key according to encrypted data [0038]. Kim teaches updating the key table according to the encrypted data (downloading a key from a database and storing the decryption key in memory) [0048] [0050].

It would have been obvious to one of ordinary skill in the art to use the decryption key update of Kim with the system of Lin, because it allows a receiver to utilize the incoming data rather than being forced to discard it.

As per claim 17, Lin teaches discarding the encrypted data when the decryption key is not stored in the key-table (packet will be discarmer if nothing located for decapsulation) [0019].

As per claim 18, Lin teaches using a Media Access Control (MAC) Address of the sender to search the key-table for the decryption key (Uses check values Key ID, Address 1, and Address 2, to search for decryption key, where Address 2 is the transmitter MAC address) [0009], [0016], [0019].

As per claim 20, Lin teaches an apparatus with a receiver controller (CPU) and Network Interface Card (Host 110, CPU, NIC) [0007] Figure 1. Lin teaches receiving encrypted data from the sender (receive encrypted packet) [0018]. Lin teaches searching a key-table of the receiver for a decryption key corresponding to the encrypted data (search for Key ID in table 1 for secret key) [0018]. Lin teaches decrypting the encrypted data through utilizing the decryption key stored in the key-table (decrypt the received packet) [0018].

Lin fails to teach updating the key-table according to the encrypted data and enabling a re-transmission mechanism of the sender when the decryption key is not stored in the key-table;

Bourk teaches enabling retransmission mechanism by not transmitting an acknowledgement from the receiver to the transmitter (Col 10 lines 25-32).

It would have been obvious to one of ordinary skill in the art to enable retransmission because of an error in decryption or errors in data transmitted.

Kim teaches searching a key table (memory) for a key according to encrypted data [0038]. Kim teaches updating the key table according to the encrypted data (downloading a key from a database and storing the decryption key in memory) [0048] [0050].

It would have been obvious to one of ordinary skill in the art to use the decryption key update of Kim with the system of Lin, because it allows a receiver to utilize the incoming data rather than being forced to discard it.

Claims 5, 12, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lin US 2005/0154871 in view of Bourk US 6,973,071 in view of Kim US 2003/0105717 in view of Jansen US 4,607,137.

As per claims 5, 12, and 19 the previous Lin-Bourk-Kim combination fails to teach replacing a least frequently used decryption key in the key-list with the decryption key transferred in.

Jansen teaches replacing a least frequently used decryption key in the key-list with the decryption key transferred in (replacing oldest key sets with new key sets) (Column 1 line 59- Column 2 line 6).

It would have been obvious to one of ordinary skill in the art to use the key replacement of Jansen with the previous Lin-Bourk-Kim combination because the newer a key is the less likely it is expired or compromised.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Akachi US 7,069,436 states decrypting data according to a key table searched by MAC address.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher J. Brown

10/3/07

